UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

KIM GREER, *individually and on behalf of all others similarly situated,* *Plaintiff,* v. POWERSCHOOL HOLDINGS, INC. and POWERSCHOOL GROUP LLC, *Defendants.*	Case No. 1:25-cv-127 **JURY TRIAL DEMAND**

CLASS ACTION COMPLAINT

Plaintiff Kim Greer, ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class") against PowerSchool Holdings, Inc. and PowerSchool Group LLC, (collectively "PowerSchool" or "Defendant"). Plaintiff alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. Plaintiff brings this class action against Defendant on behalf of herself and all other similarly situated individuals, for Defendant's failure to properly secure and safeguard personally identifiable information ("PII") including, but not limited to full names, Social Security numbers, grades, email addresses, telephone numbers, addresses, dates of birth, protected health information including medical information ("PHI") (collectively, PII and PHI are "Private Information").

2. Defendant is a national education technology firm that provides cloud-based education software for K-12 students and educators. Defendant maintains offices in the state of California.

3. To provide these services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and Class Members' Private Information.

4. As a corporation doing business in California and having employees and customers in California, Defendant is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

5. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and millions of other similarly situated persons as a result of a massive and preventable cyberattack of Defendant's networks and/or systems. On December 28, 2024, PowerSchool discovered that cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive Private Information belonging to Plaintiff and Class Members which was unprotected and unencrypted (the "Data Breach").

6. Plaintiff seeks to hold Defendant responsible for failing to ensure that Plaintiff and Class Members Private Information was maintained in a safe manner and at a minimum consistent with industry standards.

7. According to more recent announcements, Defendant admitted that "all" student and teacher data it was entrusted with, was accessed in the Data Breach.[1] Notably, PowerSchool's software is reportedly used to support more than *60 million* students across the United States.[2]

[1] WGME Staff, *PowerSchool Says All Student, Teach Data Was Accessed in Breach*, Fox23 (Jan. 17, 2025), https://fox23maine.com/news/local/powerschool-says-all-student-teacher-data-was-accessed-in-breach-maine-hack-credit-monitering; Carly Page, *PowerSchool Data Breach Victims Say Hackers Store 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/.
[2] *Id.*

8. On or around January 8, 2025, over two weeks after the Data Breach, Defendant first notified its customers, including public and private school districts throughout the United States, about the widespread Data Breach (the "Notice Letter").[3]

9. Defendant did not directly notify Plaintiff or Class Members of the Data Breach. Defendant's website or social media channels do not mention the Data Breach, or otherwise provide information for people who may have been affected.

10. However, some individual schools and districts, themselves victims of Defendant's Data Breach, made efforts to notify affected parents, students, and educators.

11. Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice Letters or observed posted notices from their current and former schools or school districts. During this time, Plaintiff and Class Members were unaware that their sensitive Private Information had been compromised, and that they were—and continue to be—at significant risk of identity theft and various other forms of personal, social, and financial harm.

12. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

13. Plaintiff and Class Members entrusted their Private Information to Defendant, directly or indirectly, with the reasonable expectation that Defendant would protect their highly sensitive data from unauthorized access and disclosure.

14. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' Private Information for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties

[3] Notice Letter (Sample), https://bloximages.newyork1.vip.townnews.com/local3news.com/content/tncms/assets/v3/editorial/e/ef/eef9dfe0-cd42-11ef-8a0d-9b6662ee1ec6/677da4657d7e6.pdf.pdf (last visited January 20, 2025).

required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' Private Information in its possession and to keep Plaintiff's and Class Members' Private Information confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

15. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' Private Information from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' Private Information.

16. Currently, the full extent of the types of Private Information, the scope of the Data Breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

17. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

18. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class

Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

19. Based on the type of sophisticated and targeted criminal activity, the type of Private Information involved, and Defendant's admission that the Private Information was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiff's and Class Members' Private Information, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' Private Information for use in future fraud and identity theft related cases.

20. As a result of Defendant's failures and the Data Breach, Plaintiff's and Class Members' identities are at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

21. Plaintiff and Class Members must now closely monitor their personal accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft. In other words, Plaintiff and Class Members are also likely to incur

out-of-pocket costs due to the Data Breach, such as purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

22. As a result of the Data Breach, Plaintiff and Class Members suffered concrete harm including, but not limited to: (i) invasion of privacy; (ii) unauthorized disclosure and/or theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempts to remediate and/or mitigate the impact of actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) actual misuse of the compromised data; (vii) nominal damages; and (viii) the substantial and imminent risk of future misuse of the compromised data, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and adequate data security measures to protect their Private Information.

23. Plaintiff brings this class action lawsuit on behalf of herself and all those similarly situated to redress harms flowing from PowerSchool's failure to adequately secure and safeguard Plaintiff's and Class Members' Private Information, and PowerSchool's failure to provide timely and adequate notice to Plaintiff and Class Members that their highly sensitive information had been improperly accessed by an unknown third party.

24. Plaintiff and Class Members have a continuing interest in ensuring their Private Information is properly safeguarded, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000

exclusive of interest and costs, and members of the proposed Class, including Plaintiff, are citizens of states different from Defendant.

26. This Court has general personal jurisdiction over Defendant PowerSchool because Defendant conducts substantial business in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

27. Venue is proper under 18 U.S.C § 1391(b)(1), (b)(1)-(2), and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

28. Plaintiff Kim Greer is a resident and citizen of Forsyth County, North Carolina. Plaintiff is a current employee of a North Carolina Public School which uses Defendant's software. Plaintiff learned from a notice emailed to her by her employer that her Private Information, including her Social Security number, was believed to be compromised in the Data Breach.[4] The notice Plaintiff received stated that

> Based on PowerSchool's analysis, an estimated 28,000 current and former [Winston-Salem/Forsyth County Schools] staff members and 150,000 current and former students were impacted by this data breach. . . For [Winston-Salem/Forsyth County Schools], social security numbers for about 16,000 [Winston-Salem/Forsyth County Schools] staff members were stolen. No student social security numbers were involved because the state does not collect that information from students. Additional data that has been breached includes names, home addresses, email addresses, and phone numbers.[5]

[4] Plaintiff Greer's Notice of Breach, attached herein as Exhibit A.

[5] *Id.*

29. Defendant PowerSchool Inc. is a corporation incorporated under the laws of the State of Delaware with its headquarters located at 150 Parkshore Drive, Folsom, Sacramento County, California 95630.

30. Defendant PowerSchool Group, LLC is a limited liability company organized under the laws of the State of Delaware with its principal address located at 150 Parkshore Drive, Folsom, Sacramento County, California 95630. PowerSchool Group, LLC is a subsidiary of PowerSchool Holdings, Inc. Defendant PowerSchool Holdings, Inc. is the parent company of PowerSchool Group, LLC and was acquired by Bain Capital in October of 2024.

31. Defendant has operated at various school districts and schools throughout the state of North Carolina, including schools within Forsyth County, North Carolina.[6]

FACTUAL ALLEGATIONS

Defendant's Business

32. PowerSchool is the largest provider of cloud-based education software for K-12 education in the country, used by more than 18,000 customers and 60 million students globally.[7]

33. On its website, Defendant touts that:

> With over 90 of the top 100 school districts in the US using PowerSchool, we simply have more experience than anyone else in implementing educational technology, providing ongoing support and training, and releasing innovative features that support schools' and districts' evolving needs. ***Partnering with PowerSchool means reducing risk by relying on the industry's most trusted and proven partner***.[8]

34. Defendant also boasts about its high standards of security, advertising: "At PowerSchool, ***we take our responsibility to protect student data privacy and to act responsibly as***

[6]https://www.powerschool.com/global/north-america/united-states/north-carolina/ (last visited Feb. 13, 2025); https://www.powerschool.com/case-studies/winston-salem-forsyth-school-district/ (last visited Feb. 13, 2025).

[7] https://www.powerschool.com/why-powerschool/?utm_medium=cpc-g (last visited Jan. 20, 2025).
[8] https://www.powerschool.com/why-powerschool/?utm_medium=cpc-g (emphasis added).

data processors to schools and districts extremely seriously. We believe ensuring the personal information contained in student education records is protected should be the standard globally and is at the center of how we build education technology at PowerSchool."[9]

35. Defendant also implicitly acknowledges the high sensitivity of the data it collects and maintains, particularly those of minor students, by explaining:

> As a signatory of the Student Privacy Pledge 2020 and holder of certifications from industry leaders such as TrustArc and Privo, PowerSchool strictly and proactively follows all legal, regulatory, and voluntary requirements for protecting student privacy including federal laws such the Family Educational Rights and Privacy Act (FERPA), the Child Online Privacy Protection Act (COPPA) and state regulations, such as California's Student Online Personal Information Protection Act (SOPIPA) and its variants.[10]

36. Contrary to those representations, however, Defendant failed to implement adequate data security measures, as evidenced by Defendant's admission of the Data Breach, which affects, to date, hundreds of thousands of individuals.

37. As a condition of providing its services, Defendant requires that its clients and users of its software—including students or parents of students and educators—supply it with Private Information.

38. As a condition of providing technology services for its clients, Defendant compiles, retains, and stores Private Information belonging to Plaintiff and Class Members.

39. On information and belief, PowerSchool maintains both the PHI and PII of its customers, including but not limited to:

a. name, residential address, phone number, and email address

b. date of birth

c. demographic information

[9] https://www.powerschool.com/blog/commitment-to-protecting-student-data-privacy/ (emphasis added)
[10] *Id.*

d. Social Security number

e. tax identification number

f. financial information

g. medication information

h. health insurance information

i. photo identification

j. employment information

k. grade information, and

l. other information that Defendant may deem necessary to provide its services.

40. Plaintiff and Class Members have entrusted Defendant, directly or indirectly, with their Private Information since its founding and Defendant has created and maintains a massive repository of Private Information belonging to millions of people, acting as a particularly lucrative target for data thieves looking to obtain, misuse, or sell Private Information.

41. In the ordinary course of its business, Defendant maintains the Private Information belonging to its customers, students, staff, current and past employees, and others.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

43. However, PowerSchool did not maintain adequate security to protect its systems from infiltration by cybercriminals.

44. Plaintiff and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely

maintained, to use such Private Information solely for business purposes, and to prevent the unauthorized disclosures of the Private Information.

45. At every step, Defendant stores Plaintiff's and Class Members' sensitive Private Information and had and continues to have a duty to protect that Private Information from unauthorized access.

46. If Plaintiff and Class Members had known that Defendant would not take reasonable and appropriate steps to protect their sensitive and valuable Private Information, they would not have entrusted it to Defendant.

The Data Breach

47. On December 28, 2024, PowerSchool purportedly first discovered that certain files on its network had been accessed and exfiltrated by an unauthorized party.[11]

48. Through its investigation, PowerSchool determined that its network and servers were subject to a cyberattack that impacted its network, thus resulting in information on its network being accessed and acquired without authorization. More specifically, PowerSchool's investigation determined that an unauthorized third-party gained access to Defendant's IT Network between December 22, 2024, and December 28, 2024 and obtained individuals' sensitive Private Information through PowerSchool's customer support portal, PowerSource.[12]

49. The investigation determined that an unauthorized third-party gained access to PowerSource by using compromised credentials.[13]

[11] *See Notice Letter*, *supra* note 2.
[12] Lawrence Abrams, PowerSchool hack exposes student, teacher data from K-12 districts (January 7, 2025) https://www.bleepingcomputer.com/news/security/powerschool-hack-exposesstudent-teacher-data-from-k-12-districts/.
[13] *Id.*

50. Upon information and belief, Defendant's investigation determined that at least the following types of Private Information were compromised in the Data Breach: name, address, phone number, Social Security number, grade point average, bus stop, password, note, alert, student ID number, parent information, and medical information.[14]

51. Furthermore, PowerSchool's investigation determined that the accessed systems contained Private Information belonging to Plaintiff and Class Members. Upon information and belief, this Private Information was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

52. While PowerSchool stated in the Notice Letter that it discovered the Data Breach on December 28, 2024, PowerSchool did not put a notice of the Data Breach on its website or send direct notice to Plaintiff or Class Members. Beginning on or around January 8, 2025, Defendant issued Notice Letters to affected schools and school districts and offered a frequently asked questions posting on its "PowerSchool Community" which is not available to Plaintiff or Class Members.

53. PowerSchool has not yet offered any type of compensation or protection to Plaintiff and Class Members.

54. Defendant had obligations created by contract, industry standards, FERPA, common law, and its own promises and representations to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

55. However, Defendant failed to take precautions designed to keep Plaintiff's and Class Members' Private Information secure.

[14] *Id.*

56. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its customers', students', and employees' Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant continues to leave significant vulnerabilities in its systems for cybercriminals to exploit and gain access to its clients', students', and employees' Private Information.

57. Plaintiff's claims arise from Defendant's failure to safeguard their Private Information and failure to provide timely notice of the Data Breach.

58. Plaintiff and Class Members relied on Defendant to: keep their Private Information confidential and securely maintained, use their Private Information for authorized purposes only, and make only authorized disclosures of this information. Plaintiff and Class Members demand that Defendant safeguard their Private Information.

59. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members.

60. Defendant cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

61. Due to PowerSchool's inadequate security measures, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

The Data Breach was Foreseeable

62. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the education services industry and other industries holding significant amounts of Private Information preceding the date of the Data Breach. In 2024 alone there were 116 confirmed ransomware attacks against educational institutions, impacting 1.8 million records.[15] Defendant knew or should have known that Plaintiff's and Class Members' Private Information Defendant maintained would be targeted by cybercriminals and ransomware attack groups.

63. Indeed, PowerSchool's website has an entire resource section on its website devoted to its Cybersecurity and Data Privacy practices and policies and offers consumers online webinars regarding best practices in securing student data.[16]

64. At all relevant times, PowerSchool knew—or should have known—that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, PowerSchool failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that PowerSchool should have anticipated and guarded against.

65. The Data Breach was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of students and employees, like Plaintiff and Class Members.

66. Additionally, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks because such warnings were readily available on the internet.

---

[15] 5 https://statescoop.com/ransomware-education-sector-decline-2024/#:~:text=The%20report%20found%20that%20educational,of%20%24847%2C000%20in%20ransom%20payments (last visited January 20, 2025).

[16] https://www.powerschool.com/resources/?filter_topics=cybersecurity-data-privacy (last visited January 20, 2025).

67. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published an online "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[17]

68. Various other governmental bodies have put entities like Defendant on notice of the likelihood of cyberattacks. In a Joint Cybersecurity Advisor, the Federal Bureau of Investigation ("FBI") and the Cybersecurity & Infrastructure Security Agency ("CISA") encouraged critical infrastructure organizations, such as Defendant, to implement their various recommendations as set forth in the advisory to reduce the likelihood and impact of inevitable ransomware and data extortion efforts by criminals and cyberhackers.[18]

69. Indeed, cyberattacks, such as the one experienced by Defendant, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, even smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[19]

70. Additionally, as companies became more dependent on computer systems to run their business,[20] *e.g.*, working remotely as a result of the Covid-19 pandemic, the danger posed by

[17] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MSISAC_Ransomware%20Guide_S508C.pdf.
[18] *See, e.g.*, *#StopRansomware: ALPHV Blackcat*, America's Cyber Defense Agency (May 10, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.
[19] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Dec. 10, 2024).
[20]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited Dec. 10, 2024).

cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[21]

71. Considering the information and guidelines readily available and accessible from the government and private technology entities before the Data Breach, Defendant—having elected to store Plaintiff's and Class Members' unencrypted Private Information in an Internet accessible environment— had reason to know that criminals and cyber hackers could likely make efforts to exfiltrate the Private Information of Plaintiff and Class Members, and that Defendant's type of business in the education sector was particularly likely to be the subject of a cyberattack.

72. Defendant knew and understood that unprotected or exposed Private Information is valuable and highly sought after by nefarious third parties seeking to illegally monetize that data through unauthorized access.

73. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and Class Members' Private Information and of the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

74. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

75. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

[21] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited Dec. 10, 2024).

76. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

77. Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Data Breaches Are Preventable

78. PowerSchool could have prevented the Data Breach by, among other things, properly encrypting or otherwise protecting its equipment, electronic record keeping systems, and computer files containing Private Information.

79. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[22]

80. PowerSchool could and should have implemented measures—as recommended by the United States Government—to prevent and detect cyberattacks and/or ransomware attacks, including, but not limited to, the following:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender

[22] Ransomware Prevention and Response, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Dec. 20, 2024).

Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations,

such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[23]

81. To prevent and detect cyberattacks and ransomware attacks, PowerSchool could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
  - remove privileged credentials
- **Thoroughly investigate and remediate alerts**

[23] *Id.*

    - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
    - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely
- **Build credential hygiene**
    - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
    - Monitor for adversarial activities
    - Hunt for brute force attempts
    - Monitor for cleanup of Event Logs
    - Analyze logon events
- **Harden infrastructure**
    - Use Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[24]

[24] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

82. Because PowerSchool collected and stored highly sensitive Private Information belonging to clients' employees and current and former students, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

83. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves accessing the Private Information of Plaintiff and hundreds of thousands of Class Members.

Defendant Failed to Comply with FTC Guidelines

84. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for businesses. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

86. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

87. The guidelines further advise businesses: not to maintain Private Information longer than necessary for authorization of a transaction; to limit access to sensitive data; to use an intrusion detection system to expose a breach as soon as it occurs; to monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and to verify that third-party service providers have implemented reasonable security measures.[25]

88. To underscore the binding significance and legal ramifications of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. These FTC enforcement actions include actions against entities who store confidential medical information (*i.e.* PHI), like Defendant.

90. Because these and similar actions were initiated prior to the Data Breach, Defendant knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Private Information.

91. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC

[25] *Id.*

publications and orders described above also form part of the basis of Defendant's duties in this regard.

92. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its clients', employees', and students' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Failed to Comply with Industry Standards

93. Experts studying cybersecurity routinely identify entities storing sensitive information like PHI and PII as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

94. Several best practices have been identified that at a minimum should be implemented, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

95. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

96. Upon information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-

2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

97. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to the cybercriminals and causing the Data Breach.

Value of Private Information

98. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[27]

99. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[28]

100. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information at the point-of-sale in a retailer data breach because, there, victims can cancel or close credit and debit card

[26] 17 C.F.R. § 248.201 (2013).
[27] *Id.*
[28] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec. 10, 2024).

accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, dates of birth, and Social Security numbers.

101. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

102. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

103. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. This is of particular concern in a case like the instant Data Breach where millions of minor children will now face risks to their identities for decades to come, and the burden of future identity monitoring will be shared by them and their parents and/or legal guardians.

104. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Data Breaches Increase Victims' Risk of Identity Theft

[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Dec. 10, 2024).

105. The unencrypted Private Information belonging to Plaintiff and Class Members will likely end up for sale on the Dark Web, because that is the *modus operandi* of hackers.

106. Unencrypted Private Information may also fall into the hands of companies that will use the detailed data for targeted marketing without the approval of Plaintiff and Class Members.

107. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the data. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

108. Plaintiff's and Class Members' Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

109. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[30]

110. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an

[30] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited Dec. 10, 2024).

astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

111. The development of "Fullz" packages means that the Private Information compromised in the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was accessed in the Data Breach, criminals may still easily create a comprehensive Fullz package and sell it—and then resell it in perpetuity—at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft & Fraud

112. Cyberattacks like the Data Breach are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

113. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[31]

114. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports

[31] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 10, 2024).

could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

115. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, in part because PowerSchool has yet to provide Plaintiff and Class Members with critical information about the Data Breach. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

116. Plaintiff's mitigation efforts are consistent with the GAO Report, which notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

117. Plaintiff's and Class Members' mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

Diminution of Value of Private Information

118. Private Information is a valuable property right.[34]

---

[32] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 10, 2024).
[33] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Dec. 10, 2024).
[34] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report") (last visited Dec. 10, 2024).

119. Sensitive PII can sell for as much as $363 per record, according to the Infosec Institute.[35]

120. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[36]

121. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[37,38]

122. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[39]

123. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

124. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if its data security systems were breached, including,

---

[35] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Dec. 10, 2024).

[37] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Dec. 10, 2024).

[38] https://datacoup.com/ (last visited Dec. 10, 2024).

[39] https://digi.me/what-is-digime/ (last visited Dec. 10, 2024).

specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

125. The fraudulent activity resulting from the Data Breach may not come to light for years.

126. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

127. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement and maintain adequate data security measures to protect Plaintiff's and Class Members' Private Information.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

128. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

129. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

130. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

131. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from the Data Breach.

Loss of Benefit of the Bargain

132. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for educational technology services—indirectly through their taxes or fees paid by their schools and school districts—Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the services and necessary data security to protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Kim Greer's Experience

133. Plaintiff Kim Greer is a current employee of Winston-Salem/Forsyth County Schools, which is a North Carolina Public School district that uses PowerSchool.

134. As a condition of her employment with this school district, Plaintiff was required to entrust PowerSchool with her Private Information.

135. Upon information and belief, at the time of the Data Breach, PowerSchool stored and maintained Plaintiff's Private Information in its systems.

136. Plaintiff received a notification from her school district informing her that over 28,00 current and former school employees were impacted in the Data Breach, and that

specifically, 16,000 Social Security numbers of current and former school employees were exfiltrated in the Data Breach.[40]

137. Plaintiff Greer is very careful about sharing her sensitive Private Information. Plaintiff Greer stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to PowerSchool had she known of PowerSchool's lax data security policies.

138. Upon information and belief, Plaintiff's Private Information was targeted, accessed, and acquired in the Data Breach.

139. As a result of the Data Breach, Plaintiff Greer made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. As described above, Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

140. Plaintiff suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of her bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as

[40] Plaintiff Greer's Notice of Breach, attached herein as Exhibit A.

Defendant's fails to undertake appropriate and adequate measures to protect her Private Information.

141. Plaintiff additionally suffered actual injury in the form of a significant increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals can easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

142. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that PowerSchool has still not informed Plaintiff of key details about the Data Breach.

143. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to continue to try to mitigate and address harms caused by the Data Breach.

144. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

145. Plaintiff Greer has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in PowerSchool's continued possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

146. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated, pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

147. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred at Defendant on or about December 5, 2024 (the "Class").

148. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

149. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

150. **Numerosity**: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, hundreds of thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records.

151. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

152. **Typicality**: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

153. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

154. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

155. **Superiority and Manageability**: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually

afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

156. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

157. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

158. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

159. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

160. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis.

161. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify Plaintiff and the Class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I

Negligence and Negligence *per se*

(On Behalf of Plaintiff and the Class)

162. Plaintiff repeats and realleges and incorporates by reference all the preceding factual allegations, as if fully set forth herein.

163. Defendant collected, stored, and maintained the Private Information of Plaintiff and the Class as part of the regular course of its business operations, which services affect commerce.

164. Plaintiff and Class Members entrusted Defendant with their Private Information with the reasonable and mutual understanding that Defendant would safeguard their information.

165. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

166. By voluntarily undertaking and assuming the responsibility to collect and store this data, in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duties included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

167. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

168. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks adequately protected the Private Information in its custody.

169. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of utilizing the education technology software provided by Defendant, and because Defendant was in a superior position to ensure that its data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

170. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above but also because Defendant is bound by industry standards to protect confidential Private Information.

171. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

172. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Plaintiff's and Class Members' Private Information it was no longer required to retain pursuant to regulations.

173. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

174. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and/or fraudulent misuse of their Private Information by third parties.

175. Defendant breached its duties, pursuant the FTC Act, industry standards, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove Plaintiff's and Class Members' Private Information it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

176. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

177. Plaintiff and Class Members are within the class of persons the FTC Act was intended to protect and the type of harm that resulted from the Data Breach is the type of harm that the statute was intended to guard against.

178. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

179. Defendant's failure to comply with relevant laws and regulations also constitutes negligence *per se*.

180. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

181. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

182. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

183. Defendant had full knowledge of the sensitivity of the Private Information it collected and stored, and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully accessed and/or disclosed.

184. Plaintiff and the Class were the foreseeable and probable victims of any inadequate data security practices and procedures. Defendant knew or should have known the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security to protect that Private Information, and the necessity of encrypting Private Information stored on Defendant's systems.

185. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

186. Plaintiff and the Class had no ability to protect their Private Information after they entrusted it to Defendant.

187. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

188. Neither Plaintiff nor Class Members contributed to the Data Breach or subsequent misuse of their Private Information as described in this Complaint.

189. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

190. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

191. There is a close causal connection between Defendant's failure to implement and maintain adequate data security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as a proximate result of Defendant's failure to exercise reasonable care in safeguarding their Private Information by adopting, implementing, and maintaining appropriate data security measures.

192. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) a significant increase in spam calls, texts, and/or emails; (vi) statutory damages;

(vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's continued possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

193. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risk of exposure of their Private Information, which remains in Defendant's continued possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

194. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

195. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring and identity theft protection services to all Class Members.

COUNT II

Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

196. Plaintiff repeats and realleges and incorporates by reference all the preceding factual allegations, as if fully set forth herein.

197. Defendant collected, stored, and maintained the Private Information of Plaintiff and the Class.

198. Plaintiff and Class Members provided their Private Information to Defendant in the ordinary course of business as a requirement to utilize the education technology software provided by Defendant. These services had monetary value to Plaintiff and Class Members, the value of which was significantly decreased as a result of Defendant's substandard data security practices.

199. Defendant offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Per the requirements to utilize the education technology software/platform administered by Defendant, Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

200. Plaintiff and Class Members entrusted Defendant with their Private Information with the reasonable and mutual understanding that Defendant would safeguard their information.

201. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of helping the schools and school districts provide education technology software to Plaintiff and Class Members.

202. When Plaintiff and Class Members provided their Private Information to Defendant for the purpose of using Defendant's education technology platform, they entered into implied contracts with Defendant.

203. Plaintiff and the Class Members, therefore, entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect their Private Information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

204. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and

regulations (including FTC guidelines on data security) and were consistent with industry standards.

205. Implicit in the agreements between Plaintiff and Class Members and Defendant, was Defendant's obligation to: (a) use such Private Information for valid business purposes only; (b) take reasonable steps to safeguard that Private Information; (c) prevent unauthorized access to and/or disclosures of the Private Information; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) retain the Private Information only under conditions that kept such information secure and confidential.

206. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

207. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

208. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

209. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable belief and expectation that Defendant would use part of those payments to obtain adequate data security. Defendant failed to do so.

210. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of an implicit assurance that Defendant would keep their Private Information secure from unauthorized access and/or disclosure.

211. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of an implied promise to monitor its computer systems and networks to ensure it adopted reasonable data security measures.

212. Every contract in this state has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

213. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

214. Defendant breached the implied contracts made with Plaintiff and the Class by failing to safeguard and protect their Private Information, by failing to delete the information once the relationship ended, and by failing to provide adequate notice to them that their Private Information was compromised as a result of the Data Breach.

215. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and continued acceptance and storage of Private Information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

216. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of

privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) a significant increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's continued possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

217. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

218. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring and identity theft protection services to all Class Members.

COUNT III

Unjust Enrichment

(On Behalf of Plaintiff and the Class)

219. Plaintiff repeats and realleges and incorporates by reference all the preceding factual allegations, as if fully set forth herein.

220. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

221. Upon information and belief, Defendant funds any data security measures it implements entirely from its general revenues, including from money they make (including that

supplied by Plaintiff's and Class Members' tax contributions to school districts) based upon representations of protecting Plaintiff's and Class Members' Private Information.

222. Thus, there is a direct nexus between money paid to Defendant and the requirement that Defendant keep Plaintiff's and Class Members' Private Information confidential and protected.

223. Plaintiff and Class Members paid Defendant a certain sum of money, or a certain sum of money was paid on their behalf by their schools and school districts, which was used to fund any data security measures implemented by Defendant.

224. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

225. Protecting the Private Information of Plaintiff and Class Members is integral to Defendant's businesses. Without their data, Defendant would be unable to provide the business services and consulting management, which comprises Defendant's core business.

226. Plaintiff's and Class Members' data and Private Information has monetary value.

227. Thus, Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, Plaintiff utilized the software, administered and operated by Defendant, and in so doing also provided Defendant with their Private Information. Defendant collected and stored the Private Information provided by Plaintiff and the Class to Defendant. In exchange, Plaintiff and Class Members should have received from Defendant the services that comprise Defendant's business and should have had their Private Information protected with adequate data security.

228. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to

it. Defendant profited from Plaintiff's and Class Members' Private Information and used Plaintiff's and Class Members' Private Information for business purposes.

229. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff and Class Members for the value that their Private Information provided.

230. Defendant acquired Plaintiff's and Class Members' Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

231. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendant or obtained services from Defendant.

232. Plaintiff and Class Members have no adequate remedy at law.

233. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security and the safety of Plaintiff's and Class Members' Private Information.

234. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

235. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) a significant increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's continued possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

236. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

237. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV

Breach of Third-Party Beneficiary Contract

(On Behalf of Plaintiff and the Class)

238. Plaintiff repeats and realleges and incorporates by reference all the preceding factual allegations, as if fully set forth herein.

239. Plaintiff and the proposed Class Members provided their Private Information to Defendant as part of using the education technology software provided by Defendant.

240. Defendant was responsible for managing and operating software, via contracts with Plaintiff and Class Members' schools and school districts.

241. Those contracts were made expressly for the benefit of Plaintiff and Class Members, whose Private Information Defendant collected, stored, and maintained, in order to operate and administer the education-technology software/platform consistent with its contractual obligations with the schools and school districts in contracted with.

242. Plaintiff and Class Members were the intended beneficiaries of the contracts entered into by Defendant and their schools and school districts—there would be no need for Defendant's services aside from the benefit to Plaintiff and Class Members. The contracts between Defendant and Plaintiff's and Class Members' school were, therefore, clearly intended for the benefit of Plaintiff and Class Members, and the benefits of those contracts were directed at Plaintiff and Class Members.

243. That Plaintiff and Class Members would rely on the contracts between Defendant and their schools and school districts to ensure the security of their Private Information was foreseeable to Defendant.

244. Defendant breached its contracts with Plaintiff's and Class Members' schools and school districts when it failed to use reasonable data security measures to adequately protect Plaintiff's and Class Members' Private Information from unauthorized access and disclosure.

245. Plaintiff and Class Members were foreseeably harmed by Defendant's failure to use reasonable data security measures, as alleged herein.

246. Accordingly, Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information, for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting Private Information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to unauthorized third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: February 20, 2025

Respectfully submitted,

/s/ David M. Wilkerson

David M. Wilkerson
NC Bar No. 35742
The Van Winkle Law Firm
11 N. Market Street
Asheville, NC 28801
(828) 258-2991
dwilkerson@vwlawfirm.com

James J. Pizzirusso* (pro hac vice forthcoming)
Nicholas U. Murphy* (pro hac vice forthcoming)
Amanda V. Boltax* (pro hac vice forthcoming)
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com
mboltax@hausfeld.com

Steven M. Nathan* (pro hac vice forthcoming)
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
(646) 357-1100
snathan@hausfeld.com

Attorneys for Plaintiff